Gmail **John Fouts <icreateupwardspirals@gmail.com>**

2025-05-20 - 10:10 P.M. EST - Re: Follow-Up on Escalated ASUS Security Case – Request for Immediate Action and Confirmation of Internal Review

1 message

John Fouts <icreateupwardspirals@gmail.com> Sat, May 10, 2025 at 10:10 PM
To: "Wendy Vu (ACI)" <wendy_vu@asus.com>
Cc: "Wendy Vu (ACI)" <wendy_vu@asus.com>

Dear Wendy Vu and ASUS Security Advisory Team,

Thank you for acknowledging the extreme seriousness and gravity of the forensic and technical evidence I have submitted to ASUS.

Your recognition formally confirms, as it should, that this is not an ordinary support issue but rather a **proven, reproducible, and corroborated case involving major cybersecurity compromise, unlawful surveillance, and cyberespionage** — all substantiated by verifiable forensic data and sustained systemic interference. As I write this message, I remain under active threat.

Given the **global scope and grave international ramifications**, I am requesting the following:

---

1. Has ASUS already submitted all prior documentation and evidence packages I've provided to your internal security team?

This includes multiple detailed reports demonstrating:

- Covert virtualization and hypervisor manipulation
- UEFI/ACPI table compromise
- Realtek media hijack vectors
- Systemic firmware-level intrusion
- Photographic evidence of motherboard components with unusual markings consistent with tampering

If any items have not yet been forwarded, I will promptly resubmit links or files as needed. I will also send the prior items directly to the security team, but need clarity on what has already been shared from your end.

2. Please confirm the name and direct contact of the individual or office leading ASUS' internal security investigation, and provide any reference ID or case number used to track this issue internally. (Identification of Case Owner / Internal Contact)

I would also appreciate knowing whether ASUS intends to involve a third-party forensic analysis firm or coordinate with relevant law enforcement or intelligence agencies.

I will be filing a formal report on my end with law enforcement, and I require ASUS' internal contact and case reference for inclusion in the report and formal legal filings.

3. Immediate escalation to ASUS upper leadership - due to the severity of this case — which has already caused:

- **Unlawful displacement and homelessness** (despite federal housing protections) - ongoing.

- **Functional disability and deterioration of medical stability - ongoing.**
- **Severe loss of access to digital infrastructure and care** for both myself and my disabled, special-needs child - ongoing.

...I am requesting **immediate escalation** of this matter to ASUS' **Executive Leadership and Board of Directors** if not already done.

I will be forwarding this message — along with all previous correspondence and supporting documentation — to:

- Chairman Jonney Shih
- Co-CEOs S.Y. Hsu and Samson Hu
- COO Joe Hsieh
- Additional Directors and Executive Officers

I respectfully request that you do the same on your end to ensure leadership level visibility of the **human rights implications and the magnitude and scale of these security failures**.

4. Law Enforcement Coordination

Please also provide the **appropriate ASUS liaison for law enforcement coordination**, including contacts for follow-up by the **U.S. Secret Service Cybersecurity Division** and/or other federal cybercrime investigators, agencies, and divisions.

This is not a speculative matter, as you are fully aware. It is a confirmed case of sustained and ongoing, reproducible sabotage and malicious system targeting.

ASUS' full engagement is crucial and critical to **halt ongoing active threats, ensure accountability for bad actors, and expose the full scope of compromise affecting hardware integrity, user safety and protection, and international digital rights**.

I am committed to full transparency and am prepared to submit all forensic evidence in a structured, validated, and secure manner.

Thank you again for your continued attention. I will next contact the ASUS Global Security Team directly per your guidance, and I respectfully ask that the requests above be treated with the **extreme urgency** this matter demands.

Respectfully,

John R. Fouts, MBA
Pro Se Whistleblower | Disabled Litigant
Phone: 502-956-0052 (Text Only)
Fax: 502-996-8246 (HIPAA Compliant)
Email: icreateupwardspirals@gmail.com

Current Temporary Location: Near the Clifton area of Louisville, KY.

On Fri, May 9, 2025 at 1:07 PM Wendy Vu (ACI) <wendy_vu@asus.com> wrote:

> Dear Mr. Fouts,
>
> Thank you for your detailed message and for taking the time to provide further clarification

regarding your concerns.

After careful review of the information you've shared, and consultation with several internal teams, we want to acknowledge the seriousness of the issues you've outlined. Given the nature of the claims and the security implications involved, we kindly ask that you direct all related correspondence, documentation, and evidence to our dedicated security team. This team is best positioned to handle matters involving potential device compromise, supply chain integrity, and cybersecurity threats. You can submit your information here: https://www.asus.com/securityadvisory/

For additional information about our security processes and how such cases are reviewed, please refer to our official Product Security Advisory page:

- https://www.asus.com/content/asus-product-security-advisory/

We appreciate your cooperation in helping us ensure the integrity and security of our products, and we thank you for bringing this matter to our attention.

Best regards,

Wendy Vu | Senior Supervisor of Customer Care

Service Department | Support Section | Corporate Customer Care

Phone: 510-739-3777 ext. 65008 | Email: Wendy_Vu@asus.com

ASUS Computer International | 48720 Kato Road, Fremont, CA 94538

From: John Fouts <icreateupwardspirals@gmail.com>
Sent: Tuesday, May 6, 2025 9:39 PM
To: Wendy Vu (ACI) <wendy_vu@asus.com>
Cc: Jennifer Stover (ACI) <Jennifer_Stover@asus.com>; ic3@fbi.gov; consumer@ftc.gov; alerts@cisa.gov; Tony Han (ACI) <Tony_Han@asus.com>; Weifen1 Liu (ACI) <Weifen1_Liu@asus.com>; legal@asus.com
Subject: 2025-05-07 - 12:08 a.m. - Subject: Follow-Up on Escalated ASUS Security Case – Legal and Technical Clarification

External email : Ensure your email is secure before opening links and attachments.

Subject: Follow-Up on Escalated ASUS Security Case – Confirmed Device Compromise

Dear Ms. Vu,

Thank you for your response and for confirming escalation to ASUS Global Research and Development.

To clarify -- once more...

This is **NOT** a standard customer support case.

This matter involves **confirmed and reproducible evidence of device compromise** across multiple ASUS products, including the TUF Gaming A16 laptop and the AX1800 and AX5400 routers.

The issues documented are **not hypothetical or "potential."**

They include:

- **Persistent firmware-level compromise** that survives factory reset
- **Remote access behaviors consistent with unauthorized control**
- **Manipulated traffic and DNS hijacking**, confirmed across clean networks
- **Hypervisor activity** not attributable to user configuration
- **Chain-of-custody and supply chain integrity failures**

These facts have been reported not only to ASUS, but also to **federal authorities**, including the:

FBI (IC3),

FTC, and

CISA,

due to the national cybersecurity implications of compromised infrastructure equipment.

I am prepared to provide the requested serial number in clearer form, of course.

However, I will not surrender these devices to ASUS without **neutral third-party forensic oversight or a federally supervised transfer**, to ensure that no evidence is altered, suppressed, or invalidated.

Further, **I strongly object to ASUS dismissing my other claims—such as damages and systemic negligence—as "outside the scope of support." These are not warranty issues.**

They are **civil, criminal, and constitutional violations**, **some of which may ultimately very likely involve ASUS as a named party in federal litigation.**

ASUS's formal participation may indeed be compelled by court order, and I reserve all rights to pursue that and any other course of action.

I expect immediate acknowledgment of:

1. ASUS's willingness to coordinate secure, traceable transfer of these devices for forensic analysis,
2. ASUS must provide **temporary replacement devices of equivalent functionality** for the duration of the investigation, so that I may maintain access to essential services (including medical) and communications.
3. Your investigation timeline and scope, and
4. The name of the internal team lead for this case, all team members, and supervisory contacts.

To further support these issues, I have attached a compiled document that includes:

- **Clear and verifiable serial number identification**
- **Forensic logs and system data** indicating persistent compromise
- **Hardware-level output** that demonstrates unauthorized firmware behavior and security violations

Please confirm receipt and advise on next steps immediately.

Sincerely,

John R. Fouts, MBA

output_compressed.pdf

On Tue, May 6, 2025 at 4:36 PM Wendy Vu (ACI) <wendy_vu@asus.com> wrote:

> Dear Mr. Fouts,
>
> Thank you for your continued communication and for submitting detailed documentation regarding your ASUS TUF Gaming A16 and AX1800, AX5400 routers. We confirm receipt of your materials and attachments.
>
> Your concerns have been formally escalated to our Global Research and Development team for internal review. Please note that this investigation may take some time, as it involves a careful and thorough technical assessment by multiple internal teams.
>
> As outlined in our warranty terms, we require that the products be returned to an ASUS Service Center for diagnostic testing. This step is essential in order to verify the reported issues and inspect the unit's condition. Once the device has been received and it is confirmed to be in its original factory state and free of any physical damage, we would be happy to consider a buyback of the unit as a potential resolution.
>
> In addition, please provide the full and clearly legible serial number (SN) of the affected device, as the images provided do not clearly display this information.
>
> We would also like to clarify the scope of our support:
>
> - Requests such as a lifetime supply of ASUS products, emergency housing, or similar forms of personal or financial support fall outside the terms and conditions of our product warranty and are not services ASUS provides.

- Additionally, ASUS will not be participating as a co-plaintiff in any litigation. If ASUS's participation is legally required, this must be pursued through proper legal channels via a valid subpoena or court order.

We remain committed to investigating this matter as appropriate, based on the facts and findings from our technical review. Your cooperation in returning the unit and providing the requested serial number will help us proceed efficiently.

If you nay have any additional questions and/or concerns, please do not hesitate to let us know.

Thank you!

Best regards,

Wendy Vu | Senior Supervisor of Customer Care

Service Department | Support Section | Corporate Customer Care

Phone: 510-739-3777 ext. 65008 | Email: Wendy_Vu@asus.com

ASUS Computer International | 48720 Kato Road, Fremont, CA 94538

From: John Fouts <icreateupwardspirals@gmail.com>
Sent: Saturday, May 3, 2025 10:29 PM
To: Wendy Vu (ACI) <wendy_vu@asus.com>; asus cc (ACI) <asus_cc@asus.com>
Cc: Jennifer Stover (ACI) <Jennifer_Stover@asus.com>; Wendy Vu (ACI) <wendy_vu@asus.com>; ic3@fbi.gov; consumer@ftc.gov; alerts@cisa.gov; Tony Han (ACI) <Tony_Han@asus.com>; Weifen1 Liu (ACI) <Weifen1_Liu@asus.com>
Subject: [WARNING: ATTACHMENT(S) MAY CONTAIN MALWARE]2025-05-04 - Subject: URGENT – Firmware Compromise Confirmed: Updated Evidence Submission + Escalation Follow-Up

External email : Ensure your email is secure before opening links and attachments.

Subject: URGENT – Firmware Compromise Confirmed: Updated Evidence Submission + Escalation Follow-Up

Hi Wendy,

Thank you again for your response. I am continuing to gather and send the materials you requested. Please see the attached for an updated set of critical documentation, including the following:

- Serial numbers and official purchase receipts for the ASUS TUF Gaming A16 and AX1800 router - AX5400 Router Receipt will be provided in near future
- Product box photos and identifying labels
- A forensic evidence archive containing ACPI firmware tables (DSDT, SSDT1–23, IVRS, TPM2, VFCT, etc.)
- Boot logs showing Secure Boot bypassed and kernel virtualization activity
- Additional screenshots and data supporting our case of firmware-level and hypervisor compromise

The latest evidence now confirms:

- **Presence of stealth hypervisor behavior in the kernel logs**, including the line: `Booting paravirtualized kernel on bare hardware`
- **Injection of Microsoft Hyper-V drivers** into a non-Hyper-V Linux environment
- **Secure Boot disabled** despite BIOS settings indicating otherwise
- **ACPI tables** such as `IVRS`, `TPM2`, and `VFCT`, and up to 23 custom `SSDT` entries with rogue identifiers (`CPMACPV7`, `CPLTFG`, `CPMDFIG2`, `GPPS_PME`, `AMDWOV`) — suggesting thermal spoofing, PCIe redirection, and virtualization payloads likely injected via firmware
- **Failure of ASUS firmware security** to protect against virtualization-layer compromise and PCIe bus deception

These facts are verifiable, reproducible, and irrefutable. I expect this to be escalated immediately to your firmware security, BIOS/UEFI development, and legal teams.

I am reiterating my original formal demands:

- A **Lifetime Protectional Contract Guarantee** and **Lifetime Supply of uncompromised equipment** for myself and my disabled child (J.A.F.)
- ASUS's participation as a **co-plaintiff in related federal litigation**
- Immediate preservation of logs, internal findings, and supply chain traceability
- A formal **Non-Retaliation Agreement**
- Compensation for the documented damages
- Coordination with federal agencies including **FTC, IC3, CISA, and HIPAA enforcement**

Attachments:

- ASUS_ACPI_evidence_bundle.zip
- ASUS 1800 router + ASUS A16 Tuf Gaming laptop receipts (PDF/JPG) - the AX5400 Receipt for that router I have not yet gotten a copy of but can send soon.
- Terminal logs and screenshots (PDF)
- `Cyber_Espionage_Legal_Notice_Meta.pdf`
- `Gmail - 2025-04-10 URGENT_ Cyber Espionage Report & Legal Notice — ADA-Protected Whistleblower Targeting.pdf`
- `EXHIBIT-EMERGENCY MEDICAL-NECESSITY-LETTER-DR-JORDAN-VAUGHN.pdf`

1. **Immediate relocation and emergency housing**, paid for by ASUS, to ensure the safety of myself and my disabled child (J.A.F.)
2. **Immediate replacement of all compromised ASUS devices**, including the TUF Gaming A16 and AX1800 router, with fully verified, uncompromised hardware
3. A **lifetime supply of top-tier, secure ASUS computing and networking equipment** for both myself and my child
4. Ongoing ASUS-based system integrity checks or trusted partner support to ensure continued protection
5. **Immediate filing by ASUS of a federal legal case** in partnership with me, listing ASUS and myself as **co-plaintiffs**
6. **Filing of a formal police report** by ASUS with:
7. Local law enforcement (Jeffersontown Police Department and Louisville Metro Police Department),
8. The Louisville FBI Field Office, local DOJ office
9. And relevant federal cybersecurity agencies (FTC, CISA, IC3, FCC),

to launch a coordinated investigation into the supply chain compromise and resulting harm

10. **A formal Lifetime Protectional Contract Guarantee** for myself and my child
11. **A Formal Non-Retaliation Agreement**
12. **Comprehensive forensic transparency**: ASUS must preserve all related internal firmware records and logs
13. Immediate preservation of logs, internal findings, and supply chain traceability
14. Compensation for the documented damages

The evidence now confirms:

- Firmware ACPI tables (`DSDT`, `SSDT1–23`, `IVRS`, `TPM2`, `VFCT`, `WSMT`) have been modified or injected with virtualization code
- Boot logs show **paravirtualized kernel activity on bare hardware**
- Secure Boot is disabled despite UEFI settings
- Microsoft Hyper-V kernel modules were **injected without consent**
- Custom ACPI identifiers (`CPMACPV7`, `CPLTFG`, `GPPS_PME`, `AMDWOV`, etc.) strongly suggest spoofed PCIe bridges and power control layers consistent with hypervisor rootkits

There is additional evidence as well that I will hold onto at this point in time

---

- final_evidence_ogr_fixed.pdf

This is not theoretical. It is **proven, forensic, and actionable**. These failures trace directly to ASUS hardware and must now be met with legal, logistical, and protective action by ASUS immediately.

These findings are irrefutable and documented across multiple forensic snapshots. I am operating with every form of communication, storage, and transmission infrastructure actively compromised. Your immediate action is required.

Please confirm:

- Receipt of the attachments
- Immediate initiation of the above actions
- Timeline for ASUS's formal response, device replacement, relocation, and legal engagement

This is a life-threatening emergency, and I am copying federal authorities to ensure this matter is recorded and escalated properly. This is a direct request for relief, protection, justice, and initial restitution.

Respectfully,

Mr. John R. Fouts, MBA
Plaintiff, Civil Rights Advocate, and Legal Guardian of J.A.F.

icreateupwardspirals@gmail.com
502-956-0052 (text only)
502-996-8246 (HIPAA Compliant)

CC:
ic3@fbi.gov
consumer@ftc.gov
alerts@cisa.gov

On Wed, Apr 30, 2025 at 6:40 PM Wendy Vu (ACI) <wendy_vu@asus.com> wrote:

Dear Mr. Fouts,

Thank you for contacting ASUS and for taking the time to share the serious concerns you've experience. We understand that you and your child are currently facing extremely difficult circumstances, including displacement and significant medical needs. Please know that we take your message seriously, and we are committed to giving your situation the careful attention and thorough review.

At ASUS, we take product security and customer safety with the utmost seriousness. Our devices are designed and manufactured to meet or exceed applicable consumer protection and cybersecurity standards, including those outlined by the Federal Trade Commission (FTC). We continually assess and improve our hardware and firmware integrity to ensure the protection of our users' privacy and data.

To initiate a formal review and escalate your case appropriately, we kindly ask that you provide the following information:

1. Serial numbers of all ASUS devices currently in your possession (e.g., the laptop and both routers),
2. Receipts or invoices confirming your original purchase of these products,
    - **<u>The receipt/invoice will need to display the:</u>**
        - • company's logo
        - • date of purchase
        - • cost
        - • serial and/or model number of ASUS product
        - • File types accepted: PDF, JPG, PNG, GIF
    - **<u>Unacceptable forms of proof of purchase are:</u>**
        - • bank statements
        - • screen shots
        - • forwarded e-mails
        - • copy & pasted e-mails
        - • do not accept files attached as TXT or RTF, DOC
3. Any supporting documentation, including forensic reports, logs, screenshots, or other evidence relating to the issues described.

We understand that gathering this information may be challenging given your current situation. If you need help identifying device serial numbers, please let us know — we are here to assist you. Once we receive this information, we will escalate the matter to our security and product investigation teams and keep you informed at each stage of the process.

Thank you for your patience and cooperation. We're committed to thoroughly reviewing your concerns.

Best regards,

Wendy Vu | Senior Supervisor of Customer Care

Service Department | Support Section | Corporate Customer Care

Phone: 510-739-3777 ext. 65008 | Email: Wendy_Vu@asus.com

ASUS Computer International | 48720 Kato Road, Fremont, CA 94538

From: John Fouts <icreateupwardspirals@gmail.com>
Sent: Tuesday, April 29, 2025 8:59 PM
To: Wendy Vu (ACI) <wendy_vu@asus.com>; Jennifer Stover (ACI) <Jennifer_Stover@asus.com>; Tony Han (ACI) <Tony_Han@asus.com>; Weifen1 Liu (ACI) <Weifen1_Liu@asus.com>; asus cc (ACI) <asus_cc@asus.com>
Cc: ic3@fbi.gov; consumer@ftc.gov; alerts@cisa.gov
Subject: 2025-04-29 - Subject: URGENT: Formal Demand for Immediate Action, Legal Partnership, and Federal Escalation

External email : Ensure your email is secure before opening links and attachments.

Dear ASUS Executive and Legal Teams,

Please find attached my formal demand letter and supporting evidence regarding catastrophic digital and physical harm enabled by ASUS-manufactured hardware.

This includes:

- A Lifetime Protectional Contract Guarantee and Lifetime Supply of top-tier equipment for both myself and my disabled child (J.A.F.), covering the remainder of our lives
- ASUS's active initiation of new federal litigation as a co-plaintiff alongside me
- Police report filing and formal escalation to federal agencies (FTC, CISA, IC3, HIPAA, NFTC)
- Preservation and delivery of logs, chain-of-custody documentation, and internal findings
- A Non-Retaliation Agreement

- Compensation for already-incurred damages, and acknowledgment of ASUS's exposure to punitive damages

This situation has involved not only the confirmed compromise of firmware-level security, stealth hypervisors, and supply chain integrity—but also real-world surveillance, unlawful displacement/forced homelessness, defamation, and federal civil rights violations.

Due to this breach, my child and I are currently displaced and surviving under severe hardship. Delivery logistics must be coordinated with me directly. I expect timely and professional response to the demands laid out in the attached letter.

I request for all communication to be in writing via email.

Contact:

- Email: icreateupwardspirals@gmail.com
- Phone: 502-956-0052 - text only
- Fax: 502-996-8246 - HIPAA compliant

Respectfully,

Mr. John R. Fouts, MBA

Plaintiff, Civil Rights Advocate, and Legal Guardian of J.A.F.

Attachment:

ASUS_Demand_Letter_and_Evidence_John_Fouts_FINAL_JAF_REMEDIES_UPDATED.pdf

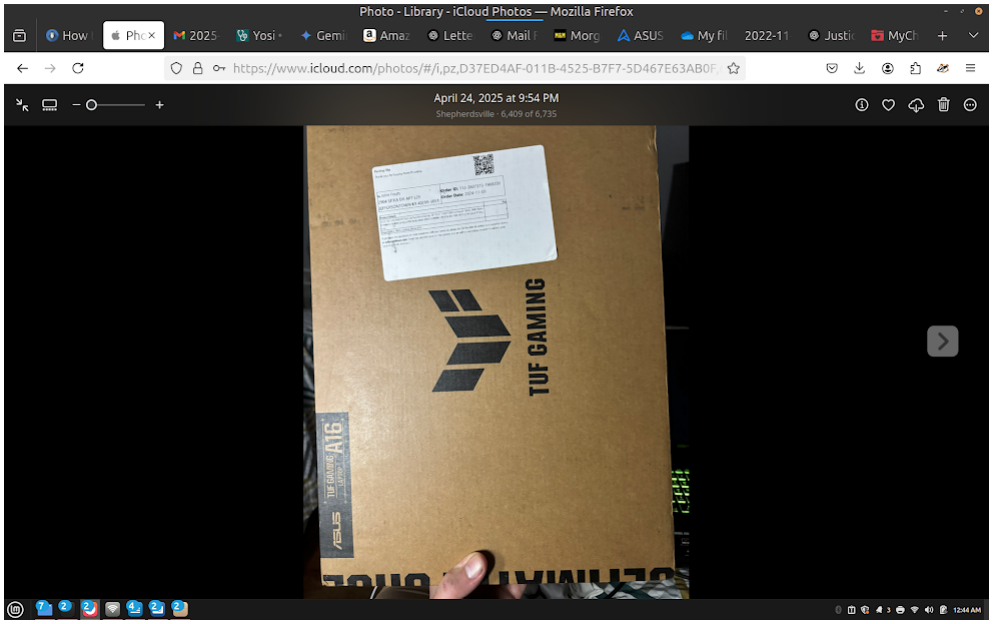


Photo - Library - iCloud Photos — Mozilla Firefox
https://www.icloud.com/photos/#/i,pz,D37ED4AF-011B-4525-B7F7-5D467E63AB0F
April 24, 2025 at 9:54 PM
Shepherdsville · 6,409 of 6,735
TUF GAMING
A16

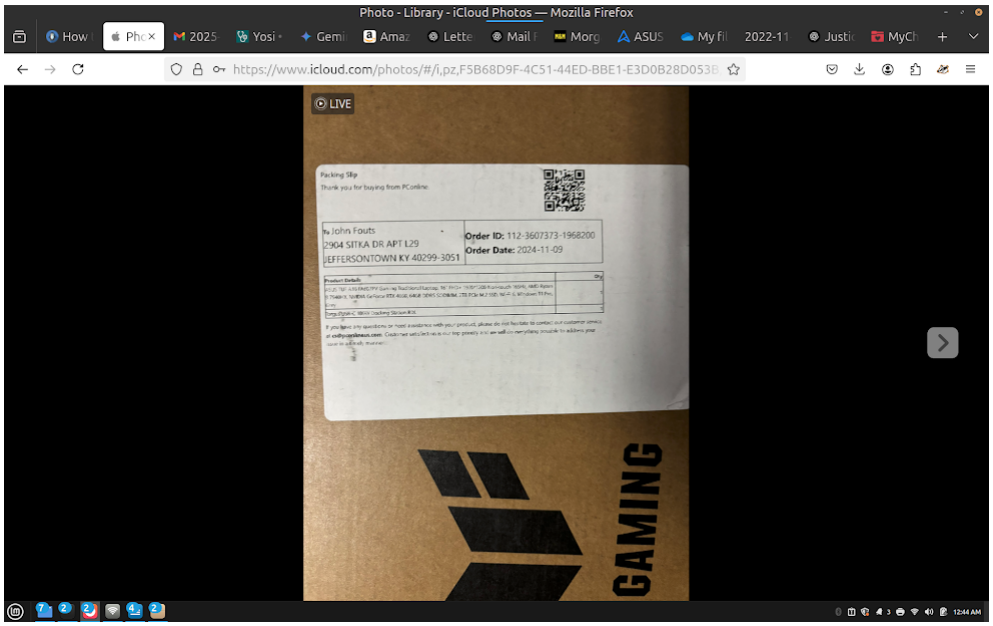


Photo - Library - iCloud Photos — Mozilla Firefox
https://www.icloud.com/photos/#/i,pz,F5B68D9F-4C51-44ED-BBE1-E3D0B28D053B
LIVE
Packing Slip
Thank you for buying from PConline.
John Fouts
2904 SITKA DR APT L29
JEFFERSONTOWN KY 40299-3051
Order ID: 112-3607373-1968200
Order Date: 2024-11-09
GAMING

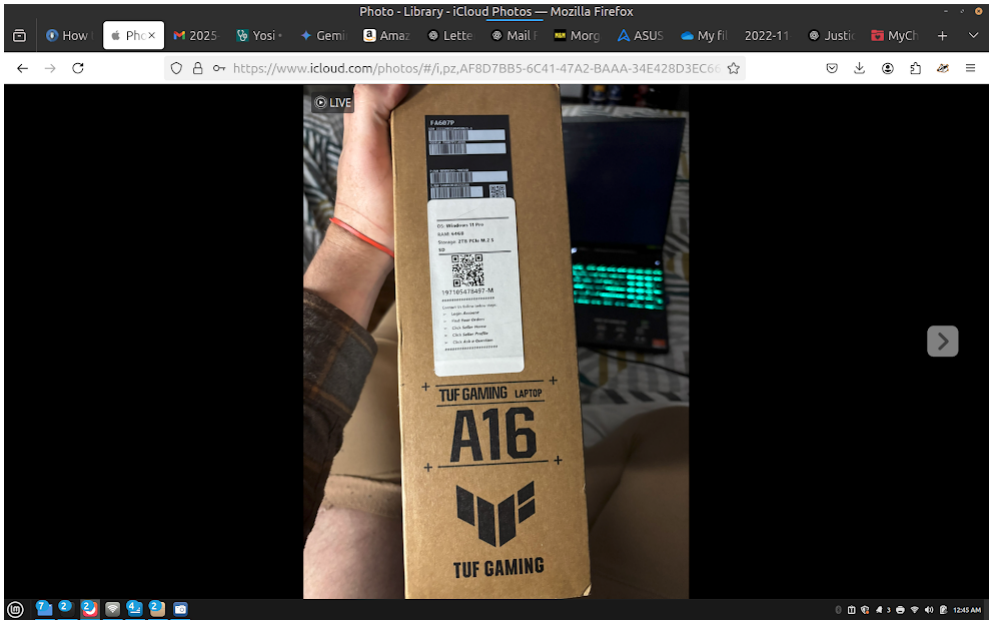


Photo - Library - iCloud Photos — Mozilla Firefox
TUF GAMING LAPTOP
A16
TUF GAMING

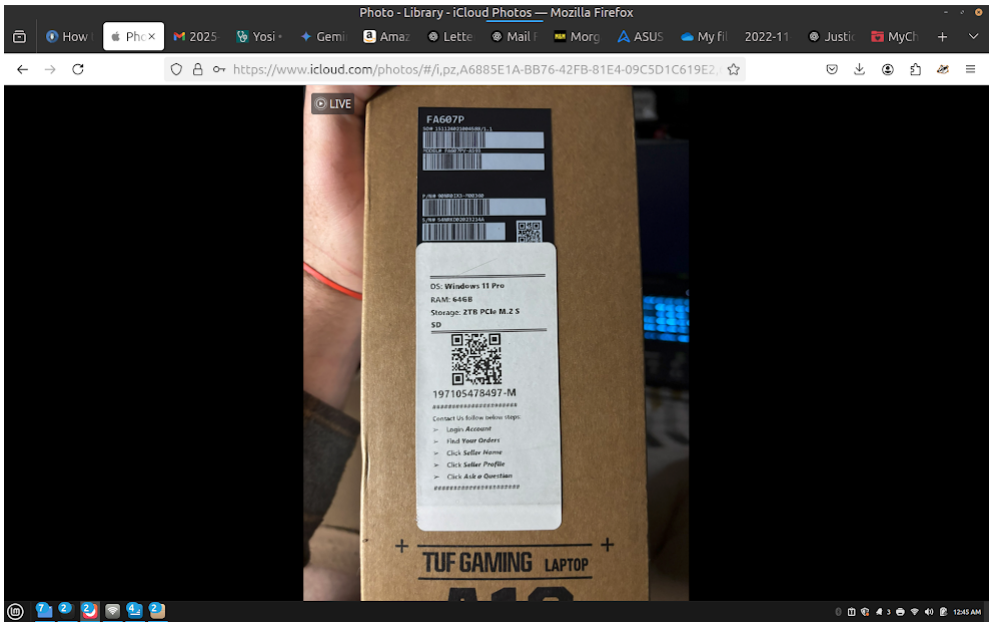


Photo - Library - iCloud Photos — Mozilla Firefox
FA607P
OS: Windows 11 Pro
RAM: 64GB
Storage: 2TB PCIe M.2 S
SD
197105478497-M
TUF GAMING LAPTOP

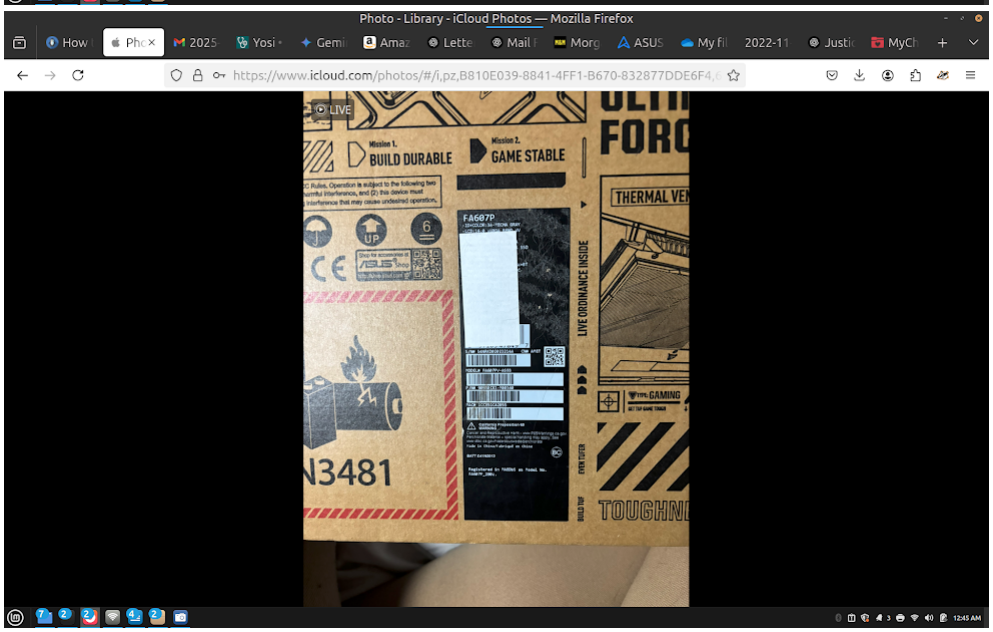
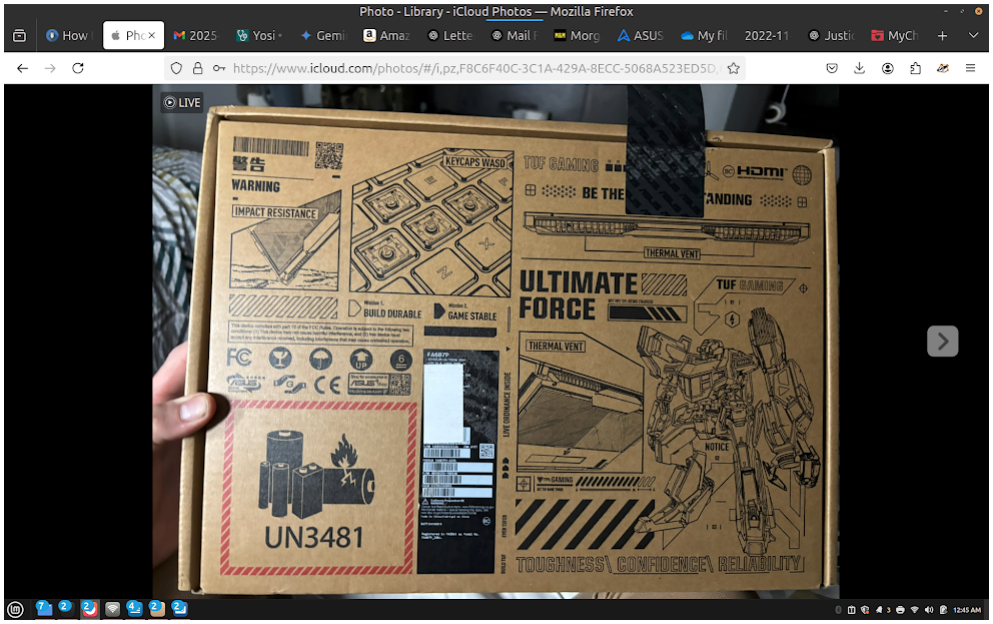
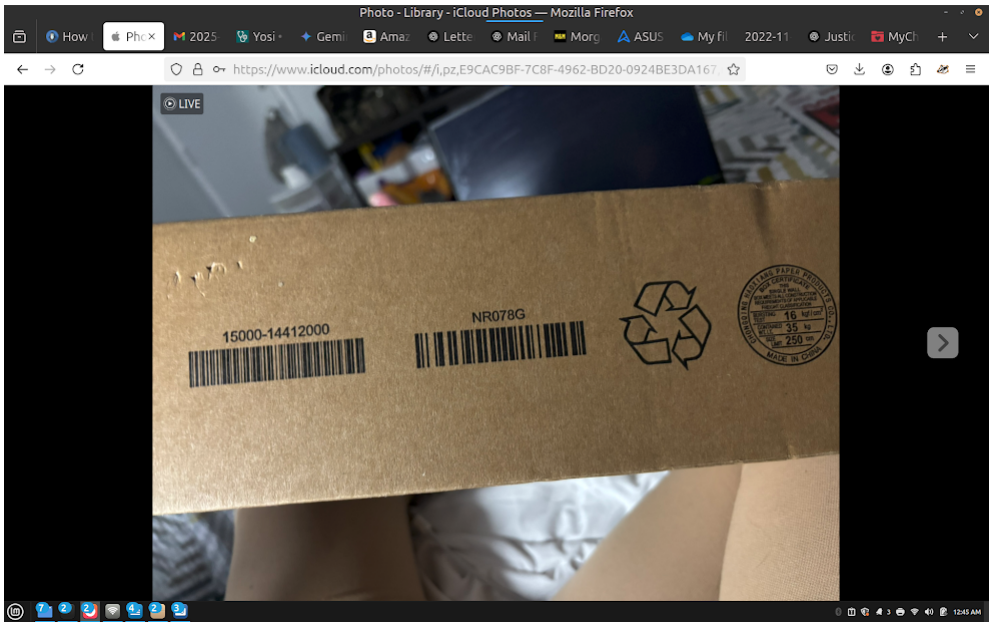


Photo - Library - iCloud Photos — Mozilla Firefox
Mission 1.
BUILD DURABLE
Mission 2.
GAME STABLE
FA607P
LIVE ORDNANCE INSIDE
N3481
TOUGHN





==========
==========
This email and any attachments to it contain confidential information and are intended solely for the use of the individual to whom it is addressed. If you are not the intended recipient or receive it accidentally, please immediately notify the sender by e-mail and delete the message and any attachments from your computer system, and destroy all hard copies. Please be advised that any unauthorized disclosure, copying, distribution or any action taken or omitted in reliance on this, is illegal and prohibited. Any views or opinions expressed are solely those of the author and do not represent those of ASUSTeK.

For pricing information, ASUS is only entitled to set a recommendation resale price. All customers are free to set their own price as they wish.
==========
==========